Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	38	(web adj site adj pages).ab.	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 11:03
L2	0	l1 and decrypt$3	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 11:03
L3	1	l1 and encrypt$3	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 11:03
L4	1	(web with pages with decrypt).ab.	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 11:04
L5	2	(applets with decrypt).ab.	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 12:06
L6	1261	((applet$2 function$2 method$2 object$2) near4 decrypt)	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 15:16
L7	381	l6 and (web adj (page HTML ASP SGML GML xml site))	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 12:08
L8	5	l7 and cryptogram	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 12:09
L9	370	l7 and key	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 12:09
L10	7	l9 and @py<"2000"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 12:20
L11	103	"5765176"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 12:20
L12	16	l11 and decrypt$3	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 12:58
L13	0	l11 and (web with page with decrypt$3)	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 12:58
L14	1	l11 and (page with decrypt$3)	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 13:19
L15	0	smart adj certificat$2 and (page with decrypt$3)	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 13:19

L16	1	(smart adj certificat$2) and decrypt$3	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 13:49
L17	279	secur$3 near4 HTML	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 13:49
L18	30	l17 and ((applet$2 function$2 method$2 object$2) near4 decrypt$3)	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 13:56
L19	15	l17 and (((applet$2 function$2 method$2 object$2) near4 decrypt$3).clm.)	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 14:01
L20	309	encrypt$3 with HTML	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 14:23
L21	19	encrypt$3 with (HTML adj form)	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 14:02
L22	3	l21 and ((applet$2 function$2 method$2 object$2) near4 decrypt)	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 14:02
L23	30110	encrypt$3 with (HTML data)	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 14:23
L24	6	encrypt$3 with (HTML adj data)	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 14:33
L25	0	obfuscat$3 with (HTML adj data)	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 14:34
L26	5	obfuscat$3 with HTML	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 14:35
L27	69	hid$4 with (HTML adj (data form))	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 14:35
L28	12	l27 and decrypt$3	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 14:59
L29	11	"5907621"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 18:04
L30	7	"6311223"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 15:10
L31	2	"6460163"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 15:14

L32	149	(sign$3 adj applet$2)	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 15:15
L33	93	l32 and HTML	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 15:15
L34	6	l33 and ((applet$2 function$2 method$2 object$2) near4 decrypt)	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 15:18
L35	9	l32 and ((applet$2 function$2 method$2 object$2) near4 decrypt)	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 15:22
L36	1261	((applet$2 function$2 method$2 object$2) near4 decrypt)	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 15:22
L37	369	l36 and (access adj control)	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 15:22
L38	115	l37 and obfuscat$3	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 15:22
L39	0	l38 and cryptogram	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 15:23
L40	111	l38 and web	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 15:24
L41	1	l40 and @py<"2000"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 15:24
L42	7	l40 and @py<"2002"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 15:25
L43	5	l40 and (plurality with key$2)	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 15:28
L44	3	l40 and HTML	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 15:54
L45	1	"6763355"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 15:55
L46	647	ullmann.in.	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 15:56
L47	1	ullmann-Lorin.in.	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 15:55

L48	0	l46 and decrypt$3	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 15:56
L49	27	l46 and HTML	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 15:56
L50	0	l49 and encrypt$3	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 15:56
L51	32	l46 and hid$4	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 15:57
L52	6	l49 and hid$4	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 15:58
L53	14	"6105012"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 15:58
L54	10	l53 and decrypt$3	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 15:58
L55	0	self-decrypt.ti.	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 18:04
L56	5	self-decrypt$3.ti.	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 18:06
L57	28	"6052780"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 18:06
L58	7	l57 and HTML	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 18:09
L59	157	(encrypt$3 with event$7).clm.	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 18:10
L60	47	l59 and web	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 18:10
L61	9	l59 and (web.clm.)	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 18:36
L62	704	sandbox	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 18:36
L63	284	l62 and java	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 18:41

L64	32	l63 and (download$4 with object)	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 18:37
L65	1	l64 and obfuscat$3	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 18:37
L66	15	l64 and decrypt$3	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 18:38
L67	136	l62 and HTML	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 18:41
L68	114	l67 and download$4	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 18:42
L69	6	l68 and obfuscat$3	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 18:43
L70	37	l68 and decrypt$3	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 18:48
L71	0	((crypto$4 adj key) same (bytecode with obfuscat$3)).ab.	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 18:48
L72	0	((crypto$4 adj key) same (bytecode with obfuscat$3))	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 18:48
L73	0	((crypto$6 with key) same (bytecode with obfuscat$3))	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 18:49
L74	3	((crypto$6 with key) same bytecode)	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 18:51
L75	18	((crypto$6 with key) same obfuscat$3)	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 18:51
L76	16	l75 and decrypt$3	US-PGPUB; USPAT; EPO; JPO	OR	ON	2005/05/10 18:52

PORTAL USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: The ACM Digital Library The Guide

cryptogram

SEARCH

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Term used **cryptogram** Found **39** of **154,226**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 39 Result page: **1** 2 next

Relevance scale

1 To decode short cryptograms

George W. Hart

September 1994 **Communications of the ACM**, Volume 37 Issue 9

Full text available: pdf(3.37 MB) Additional Information: full citation, references, citings, index terms

2 Cryptology in Transition

Abraham Lempel

December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4

Full text available: pdf(1.63 MB) Additional Information: full citation, references, citings, index terms

3 Hardware protection against software piracy

Tim Maude, Derwent Maude

September 1984 **Communications of the ACM**, Volume 27 Issue 9

Full text available: pdf(843.02 KB) Additional Information: full citation, abstract, references, citings, index terms

A system that prevents illicit duplication of proprietary software is suggested. It entails the customization of the programs for each computer by encryption. The use of a public key cryptogram for this purpose means that anyone can customize programs, but neither other programmers nor the people having complete access to the target computer can obtain copies that will run on other machines. A possible implementation of the system is considered in some detail. It is based on a hardware secu ...

Keywords: proprietary software protection, public key cryptography, software encryption, software piracy

4 Authentication codes that are r-fold secure against spoofing

L. Tombak, R. Safavi-Naini

November 1994 **Proceedings of the 2nd ACM Conference on Computer and communications security**

Full text available: pdf(373.06 KB) Additional Information: full citation, abstract, references, index terms

In this paper we study authentication codes (A-codes) that are r-fold secure against

spoofing. We obtain necessary and sufficient conditions for such codes and give a characterization of codes with a minimum number of encoding rules. We will show that if the source is uniform, A-codes that provide perfect protection against spoofing attack of order r are r-fold secure.

Keywords: r-fold security, authentication, authentication codes, computer security, cryptography

5 Computer security (SEC): Protected transmission of biometric user authentication data for oncard-matching

Ulrich Waldmann, Dirk Scheuermann, Claudia Eckert
March 2004 **Proceedings of the 2004 ACM symposium on Applied computing**

Full text available: pdf(574.45 KB) Additional Information: full citation, abstract, references

Since fingerprint data are no secrets but of public nature, the verification data transmitted to a smartcard for oncard-matching need protection by appropriate means in order to assure data origin in the biometric sensor and to prevent bypassing the sensor. For this purpose, the verification data to be transferred to the user smartcard is protected with a cryptographic checksum that is calculated within a separate security module controlled by a tamper resistant card terminal with integrated bio ...

Keywords: authentication, biometrics, cryptographic protocols, data integrity, electronic signature, oncard-matching, smartcards, system security, tamper proof environment

6 A model to order the encryption algorithms according to their quality

A. R. Prieto, J. G. Tomas
July 1987 **ACM SIGCOMM Computer Communication Review**, Volume 17 Issue 3

Full text available: pdf(565.17 KB) Additional Information: full citation, abstract, index terms

Usually the unicity distance is used to give the strength of encryption algorithms. In this work, the behaviour of encipherment algorithm has been analyzed and two different parameters are proposed in order to evaluate the quality. These parameters are checked against the unicity distance and a final test has been executed, using DES.

7 Secure communications over insecure channels

Ralph C. Merkle
April 1978 **Communications of the ACM**, Volume 21 Issue 4

Full text available: pdf(597.27 KB) Additional Information: full citation, abstract, references, citings, index terms

According to traditional conceptions of cryptographic security, it is necessary to transmit a key, by secret means, before encrypted massages can be sent securely. This paper shows that it is possible to select a key over open communications channels in such a fashion that communications security can be maintained. A method is described which forces any enemy to expend an amount of work which increases as the square of the work required of the two communicants to select the key. The method ...

Keywords: communications security, computer network security, cryptography, cryptology, key distribution, passive eavesdropping, public key cryptosystem, security, wiretap

8 ACM Forum: letters

March 1976 **Communications of the ACM**, Volume 19 Issue 3

Full text available: pdf(534.00 KB) Additional Information: full citation, references

9 Signature simulation and certain cryptographic codes
Carl Hammer
January 1971 **Communications of the ACM**, Volume 14 Issue 1

Full text available: pdf(1.51 MB) Additional Information: full citation, abstract, references

Three cyphers allegedly authored by Thomas Jefferson Beale in 1822 have been the subject of intensive study for over 100 years. Generations of cryptanalysts have expended untold man-years, thus far without success, attempting to decode them; vast armies of fortune hunters and treasure seekers have devoted Herculean labors to digging up the rolling hills of Virginia trying to locate the promised bonanza. The history of pertinent activities would fill volumes, yet serious students of cryptogr ...

Keywords: Declaration of Independence, Magna Carta, Thomas Jefferson Beale, codes, cryptanalysis, cyphers, decoding, encoding, pseudotext, signature, simulation

10 Some Open Problems In Cryptography
C. Leung
December 1978 **Proceedings of the 1978 annual conference**

Full text available: pdf(427.01 KB) Additional Information: full citation, abstract, references, index terms

In the past, cryptography has been mainly concerned with the problem of private communication between two parties. A number of ciphers exist which solve this problem more or less satisfactorily. One common factor behind these ciphers is the use of certain secret keys. With the advent of commercial data networks, there is a need for many pairs of users to communicate in privacy. The classical method of distributing secret keys (over a secure channel) to each user pair becomes very expensive ...

Keywords: Complexity, Cryptography, Key distribution, Security

11 SIGCOMM 1- Software-hardware interactions: An experimental application of cryptography to a remotely accessed data system
J. L. Smith, W. A. Notz, P. R. Osseck
August 1972 **Proceedings of the ACM annual conference - Volume 1**

Full text available: pdf(1.46 MB) Additional Information: full citation, abstract, references, citings

An experimental system has been developed which illustrates ways cryptography can be applied to certain data-security problems concerning remotely accessible data files. These problems are in two main classes: security of data while in transit over communications lines and security of data while in storage. The system makes use of a combination of software and special hardware to provide enciphering and deciphering of messages between a terminal and a data processor. Not only is the content of m ...

Keywords: communication security, cryptography, data communications, data security, data-base protection, file protection, teleprocessing, terminals authentication, time-shared systems

12 Threshold-based identity recovery for privacy enhanced applications
Joachim Biskup, Ulrich Flegel
November 2000 **Proceedings of the 7th ACM conference on Computer and**

communications security

Full text available: pdf(332.52 KB) Additional Information: full citation, references, index terms

Keywords: anonymity, privacy, pseudonymity, purpose binding, secret sharing

13 A computer ethics course

Ronald S. King, James H. Nolen

March 1985 **ACM SIGCSE Bulletin , Proceedings of the sixteenth SIGCSE technical symposium on Computer science education**, Volume 17 Issue 1

Full text available: pdf(559.40 KB) Additional Information: full citation, references, citings, index terms

14 Security: Key-assignment strategies for CPPM

André Adelsbach, Jörg Schwenk

September 2004 **Proceedings of the 2004 multimedia and security workshop on Multimedia and security**

Full text available: pdf(454.53 KB) Additional Information: full citation, abstract, references, index terms

CSS, the first system to protect multimedia content on the new DVD medium failed badly, because both its encryption algorithm and its key management could easily be broken. A new industry initiative, the 4C Entity, LLC (founded by IBM, Intel, Matsushita and Toshiba), presents a more mature approach, called "Copy Protection for Prerecorded Media" (CPPM), which has already been adopted in DVD-Audio.A key-feature of CPPM is its advanced key-management, which allows for system renewability by revoki ...

Keywords: CPPM, content protection, device revocation, key-assignment, key-management

15 Designing and implementing a cyberwar laboratory exercise for a computer security course

Paul J. Wagner, Jason M. Wudi

March 2004 **ACM SIGCSE Bulletin , Proceedings of the 35th SIGCSE technical symposium on Computer science education**, Volume 36 Issue 1

Full text available: pdf(191.77 KB) Additional Information: full citation, abstract, references, index terms

The development of a cyberwar laboratory exercise for a computer security course raises many pedagogical and management issues relating to the structure of the laboratory, its network and the exercise itself. We have designed, implemented and given such an exercise, and faced many of these issues. Evaluation of this exercise leads to multiple insights about the proper goals, structure and implementation of such an exercise.

Keywords: cybersecurity, cyberwar, exercise, laboratory, security

16 Automatic text indexing using complex identifiers

Gerald Salton

January 2000 **Proceedings of the ACM conference on Document processing systems**

Full text available: pdf(569.46 KB) Additional Information: full citation, references, citings, index terms

17

Tablet: personal computer of the year 2000
B. W. Mel, S. M. Omohundro, A. D. Robison, S. S. Skiena, K. H. Thearling
June 1988 **Communications of the ACM**, Volume 31 Issue 6

Full text available: pdf(1.67 MB) Additional Information: full citation, abstract, references, citings, index terms

A design represents a compromise between conflicting goals, and the design of the personal computer of the year 2000 is no exception. We seek something that will fit comfortably into people's lives while dramatically changing them. This may appear to be a contradiction that cannot be reconciled. But if the technology does not fit easily into the habits and lifestyles of its human users, it will be discarded by those it was meant to help. And if this new tool does not change the life of its ...

18 A user authentication scheme not requiring secrecy in the computer
Arthur Evans, Edwin Weiss
August 1974 **Communications of the ACM**, Volume 17 Issue 8

Full text available: pdf(592.31 KB) Additional Information: full citation, abstract, references, citings, index terms

In many computer operating systems a user authenticates himself by entering a secret password known solely to himself and the system. The system compares this password with one recorded in a Password Table which is available to only the authentication program. The integrity of the system depends on keeping the table secret. In this paper a password scheme is presented which does not require secrecy in the computer. All aspects of the system, including all relevant code and ...

Keywords: authentication, cryptology, one-way encryption, operating system security, passwords, security

19 A Study of Methods for Systematically Abbreviating English Words and Names
Charles P. Bourne, Donald F. Ford
October 1961 **Journal of the ACM (JACM)**, Volume 8 Issue 4

Full text available: pdf(641.41 KB) Additional Information: full citation, abstract, references, citings, index terms

This study investigated various techniques for systematically abbreviating English words and names. Most of the attention was given to the techniques which could be mechanized with a digital device such as a general purpose digital computer. Particular attention was paid to techniques that could process incoming information without prior knowledge of its existence (i.e., no table lookups). Thirteen basic techniques and their modifications are described. In addition, most of the techniques w ...

20 Documentation: Effective AND literate
Paul S Burdett
February 1986 **Proceedings of the 4th annual international conference on Systems documentation**

Full text available: pdf(391.69 KB) Additional Information: full citation, abstract, references, index terms

The purpose of this paper is to show how documentation can be literate, in a stylistic sense, and still be effective. Literate prose is a powerful tool that, when properly used in computer documentation, can take advantage of the full power of the English language. This does not mean that all computer documentation must or can read like a Nobel Prize novel, but neither does it have to read like a military cryptogram. A happy medium — founded on healthy grammar and syntax, and followin ...

Results 1 - 20 of 39 Result page: **1** 2 next

ACM Portal is published by the Association for Computing Machinery. Copyright © 2005 ACM, Inc.
Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player

PORTAL
USPTO
Subscribe (Full Service) Register (Limited Service, Free) Login
Search: The ACM Digital Library The Guide
decrypt web page
THE ACM DIGITAL LIBRARY
Feedback Report a problem Satisfaction survey

Terms used **decrypt web page** Found **20,165** of **154,226**

Sort results by: publication date
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 161 - 180 of 200 Result page: previous 1 2 3 4 5 6 7 8 **9** 10 next
Best 200 shown Relevance scale

161 Emulators of "historic machines"
John A. N. Lee
June 2000 **ACM SIGCSE Bulletin**, Volume 32 Issue 2
Full text available: pdf(310.84 KB) Additional Information: full citation, index terms

162 Columns: Risks to the public in computers and related systems
Peter G. Neumann
May 2000 **ACM SIGSOFT Software Engineering Notes**, Volume 25 Issue 3
Full text available: pdf(1.11 MB) Additional Information: full citation

163 Software engineering for security: a roadmap
Premkumar T. Devanbu, Stuart Stubblebine
May 2000 **Proceedings of the Conference on The Future of Software Engineering**
Full text available: pdf(1.71 MB) Additional Information: full citation, references, citings, index terms

Keywords: copy protection, security, software engineering, water-marking

164 Implementing a caching service a distributed COBRA objects
Gregory V. Chockler, Danny Dolev, Roy Friedman, Roman Vitenberg
April 2000 **IFIP/ACM International Conference on Distributed systems platforms**
Full text available: pdf(324.53 KB) Additional Information: full citation, abstract, references, citings

This paper discusses the implementation of CASCADE, a distributed caching service for CORBA objects. Our caching service is fully CORBA compliant, and supports caching of active objects, which include both data and code. It is specifically designed to operate over the Internet by employing a dynamically built cache hierarchy. The service architecture is highly configurable with regard to a broad spectrum of application parameters. The main benefits of CASCADE are enhanced availability and ser

165 Compensating for a lack of transparency

Berry Schoenmakers
April 2000 **Proceedings of the tenth conference on Computers, freedom and privacy: challenging the assumptions**
Full text available: pdf(47.18 KB) Additional Information: full citation, references, index terms

166 Linux DVD Update
Craig Knudsen
March 2000 **Linux Journal**
Full text available: html(6.52 KB) Additional Information: full citation, abstract, references, index terms

Watching movies is a favorite leisure-time activity for many people. Today you can watch movies on your laptop computer as well as your TV screen. But can you do it with Linux?

167 The evolution of the DARWIN system
Joan D. Walton, Robert E. Filman, David J. Korsmeyer
March 2000 **Proceedings of the 2000 ACM symposium on Applied computing**
Full text available: pdf(897.54 KB) Additional Information: full citation, references, index terms

Keywords: DARWIN, WWW applications, collaborative engineering, distributed analysis, wind-tunnel

168 Linux and open-source applications
Peter Jones, M. B. Jorgenson
February 2000 **Linux Journal**
Full text available: html(20.48 KB) Additional Information: full citation, abstract, references, index terms

The building blocks for a secu

169 Authentication primitives and their compilation
Martín Abadi, Cédric Fournet, Georges Gonthier
January 2000 **Proceedings of the 27th ACM SIGPLAN-SIGACT symposium on Principles of programming languages**
Full text available: pdf(1.55 MB) Additional Information: full citation, abstract, references, citings, index terms

Adopting a programming-language perspective, we study the problem of implementing authentication in a distributed system. We define a process calculus with constructs for authentication and show how this calculus can be translated to a lower-level language using marshaling, multiplexing, and cryptographic protocols. Authentication serves for identity-based security in the source language and enables simplifications in the translation. We reason about correctness relying on the concepts of o ...

170 Workings of a Virtual Private Network in Linux--Part 2: More about securing our commminication with the Internet
David Morgan
January 2000 **Linux Journal**
Full text available: html(23.81 KB) Additional Information: full citation, references, index terms

171 Separating key management from file system security

David Mazières, Michael Kaminsky, M. Frans Kaashoek, Emmett Witchel
December 1999 **ACM SIGOPS Operating Systems Review , Proceedings of the seventeenth ACM symposium on Operating systems principles**, Volume 33 Issue 5

Full text available: pdf(1.77 MB) Additional Information: full citation, abstract, references, citings, index terms

No secure network file system has ever grown to span the Internet. Existing systems all lack adequate key management for security at a global scale. Given the diversity of the Internet, any particular mechanism a file system employs to manage keys will fail to support many types of use.We propose separating key management from file system security, letting the world share a single global file system no matter how individuals manage keys. We present SFS, a secure file system that avoids internal ...

172 Workings of a Virtual Private Network, Part 1: A look into VPNs--what they are and how they work
David Morgan
December 1999 **Linux Journal**

Full text available: html(20.51 KB) Additional Information: full citation, references, index terms

173 Nark: receiver-based multicast non-repudiation and key management
Bob Briscoe, Ian Fairman
November 1999 **Proceedings of the 1st ACM conference on Electronic commerce**

Full text available: pdf(168.86 KB) Additional Information: full citation, references, citings, index terms

Keywords: Internet, audit trail, key management, multicast, non-repudiation, smartcard, watermark

174 On secure and pseudonymous client-relationships with multiple servers
Eran Gabber, Phillip B. Gibbons, David M. Kristol, Yossi Matias, Alain Mayer
November 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 4

Full text available: pdf(161.56 KB) Additional Information: full citation, abstract, references, citings, index terms, review

This paper introduces a cryptographic engine, Janus, which assists clients in establishing and maintaining secure and pseudonymous relationships with multiple servers. The setting is such that clients reside on a particular subnet (e.g., corporate intranet, ISP) and the servers reside anywhere on the Internet. The Janus engine allows each client-server relationship to use either weak or strong authentication on each interaction. At the same time, each interaction preserves privacy by neithe ...

Keywords: Janus function, anonymity, mailbox, persistent relationship, privacy, pseudonym

175 Password hardening based on keystroke dynamics
Fabian Monrose, Michael K. Reiter, Susanne Wetzel
November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**

Full text available: pdf(1.01 MB) Additional Information: full citation, abstract, references, citings, index terms

We present a novel approach to improving the security of passwords. In our approach, the legitimate user's typing patterns (e.g., durations of keystrokes, and latencies between keystrokes) are combined with the user's password to generate a hardened password that is convincingly more secure than conventional passwords against both online and offline attackers. In addition, our scheme automatically adapts to gradual changes in a user's typing patterns while maintaining the s ...

176 Who's got the key?
David Henry
November 1999 **Proceedings of the 27th annual ACM SIGUCCS conference on User services: Mile high expectations**
Full text available: pdf(30.32 KB) Additional Information: full citation, references, index terms

Keywords: PKI, certificate authority, encryption

177 RBAC on the Web by smart certificates
Joon S. Park, Ravi Sandhu
October 1999 **Proceedings of the fourth ACM workshop on Role-based access control**
Full text available: pdf(867.12 KB) Additional Information: full citation, references, citings, index terms

178 Confined types
Jan Vitek, Boris Bokowski
October 1999 **ACM SIGPLAN Notices , Proceedings of the 14th ACM SIGPLAN conference on Object-oriented programming, systems, languages, and applications**, Volume 34 Issue 10
Full text available: pdf(1.71 MB) Additional Information: full citation, abstract, references, citings, index terms

Sharing and transfer of object references is difficult to control in object-oriented languages. Unconstrained sharing poses serious problems for writing secure components in object-oriented languages. In this paper, we present a set of inexpensive syntactic constraints that strengthen encapsulation in object-oriented programs and facilitate the implementation of secure systems. We introduce two mechanisms: confined types to impose static scoping on dynamic object references ...

179 Analysis and development of Java Grande benchmarks
J. A. Mathew, P. D. Coddington, K. A. Hawick
June 1999 **Proceedings of the ACM 1999 conference on Java Grande**
Full text available: pdf(1.07 MB) Additional Information: full citation, references, citings, index terms

Keywords: Java, Java Grande, benchmarks

180 Cryptography on the Internet
Jeff Zadeh
April 1999 **Proceedings of the 37th annual Southeast regional conference (CD-ROM)**
Full text available: pdf(26.43 KB) Additional Information: full citation, index terms

Results 161 - 180 of 200 Result page: previous 1 2 3 4 5 6 7 8 **9** 10 next

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2005 ACM, Inc.
Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player

PORTAL USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: The ACM Digital Library The Guide

decrypt web page

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used **decrypt web page** Found **20,165** of **154,226**

Sort results by: publication date

Display results: expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 181 - 200 of 200 Result page: previous 1 2 3 4 5 6 7 8 9 **10**

Best 200 shown Relevance scale

181 Emperor: cheap legal secure cryptography for the Web

Clifton Davis, Christoph F. Eick

February 1999 **Proceedings of the 1999 ACM symposium on Applied computing**

Full text available: pdf(864.94 KB) Additional Information: full citation, references, index terms

Keywords: Web security, distributed source cryptography, electronic commerce, public key cryptography

182 Consistent, yet anonymous, Web access with LPWA

Eran Gabber, Phillip B. Gibbons, David M. Kristol, Yossi Matias, Alain Mayer

February 1999 **Communications of the ACM**, Volume 42 Issue 2

Full text available: pdf(207.80 KB) html(30.92 KB) Additional Information: full citation, references, citings, index terms

183 DeepView: a channel for distributed microscopy and informatics

B. Parvin, J. Taylor, G. Cong, M. A. OKeefe, M. H. Barcellos-Hoff

January 1999 **Proceedings of the 1999 ACM/IEEE conference on Supercomputing (CDROM)**

Full text available: pdf(2.69 MB) Additional Information: full citation, references, citings, index terms

184 Simulation and C41 data collection in support of force XXI training

William J. Frederic, Mark B. Hamby, James S. Mathison, Ronald D. Nugen

December 1998 **Proceedings of the 30th conference on Winter simulation**

Full text available: pdf(1.07 MB) Additional Information: full citation, index terms

185 Data security for Web-based CAD

Scott Hauck, Stephen Knol

May 1998 **Proceedings of the 35th annual conference on Design automation - Volume**

00

Full text available: pdf(198.79 KB) Publisher Site Additional Information: full citation, abstract, references, citings, index terms

Internet-based computing has significant potential for improving most high-performance computing, including VLSI CAD. In this paper we consider the ramifications of the Internet on electronics design, and develop two models for Web-based CAD. We also investigate the security of these systems, and propose methods for protection against threats both from unrelated users, as well as from the CAD tools and tool developers themselves. These techniques provide methods for hiding unnecessary infor ...

Keywords: Internet, Web-based CAD, data security, encryption

186 Cluster-based scalable network services

Armando Fox, Steven D. Gribble, Yatin Chawathe, Eric A. Brewer, Paul Gauthier

October 1997 **ACM SIGOPS Operating Systems Review , Proceedings of the sixteenth ACM symposium on Operating systems principles**, Volume 31 Issue 5

Full text available: pdf(2.42 MB) Additional Information: full citation, references, citings, index terms

187 Secure distribution of watermarked images for a digital library of ancient papers

Christian Rauber, Joe Ó Ruanaidh, Thierry Pun

July 1997 **Proceedings of the second ACM international conference on Digital libraries**

Full text available: pdf(1.13 MB) Additional Information: full citation, references, citings, index terms

188 Open Location

Tom Jewett

June 1997 **ACM SIGCAS Computers and Society**, Volume 27 Issue 2

Full text available: pdf(283.83 KB) Additional Information: full citation

189 World Wide Web based grades management

Atsuyuki Morishima, Hiroyuki Kitagawa

April 1997 **Proceedings of the 1997 ACM symposium on Applied computing**

Full text available: pdf(388.64 KB) Additional Information: full citation, index terms

Keywords: Internet, JAVA, class management, grading system

190 Teaching ethical and social issues in CS1 and CS2

Kay G. Schulze, Frances S. Grodzinsky

March 1997 **ACM SIGCSE Bulletin , Proceedings of the twenty-eighth SIGCSE technical symposium on Computer science education**, Volume 29 Issue 1

Full text available: pdf(498.54 KB) Additional Information: full citation, abstract, references, citings, index terms

The discussion of whether ethical and social issues of computing should be explored in undergraduate computer science education has resulted in most academic institutions and

educators agreeing that they are important topics that must be included. Further support has been provided by Curricula '91 [16], the CSAC/CSAB accreditation [2] and ImpactCS [12]. Many books [7, 8, 9, 10] and papers [6, 14] have discussed what topics should be covered and what techniques can be used either in a dedicated c ...

191 Supporting multi-user, multi-applet workspaces in CBE
Jang Ho Lee, Atul Prakash, Trent Jaeger, Gwobaw Wu
November 1996 **Proceedings of the 1996 ACM conference on Computer supported cooperative work**
Full text available: pdf(1.47 MB) Additional Information: full citation, references, citings, index terms

Keywords: CSCW toolkits, DistView, Web-based collaboration, access control, group communication, groupware, shared electronic workspaces

192 Security on the move: indirect authentication using Kerberos
Armando Fox, Steven D. Gribble
November 1996 **Proceedings of the 2nd annual international conference on Mobile computing and networking**
Full text available: pdf(1.34 MB) Additional Information: full citation, references, citings, index terms

193 Providing education electronically to nontraditional sites: new delivery to a new audience
Nancy C. McAllister, David F. McAllister
October 1996 **Proceedings of the 14th annual international conference on Systems documentation: Marshaling new technological forces: building a corporate, academic, and user-oriented triangle**
Full text available: pdf(777.73 KB) Additional Information: full citation, references, index terms

194 The structure and performance of interpreters
Theodore H. Romer, Dennis Lee, Geoffrey M. Voelker, Alec Wolman, Wayne A. Wong, Jean-Loup Baer, Brian N. Bershad, Henry M. Levy
September 1996 **Proceedings of the seventh international conference on Architectural support for programming languages and operating systems**, Volume 31 , 30 Issue 9 , 5
Full text available: pdf(1.17 MB) Additional Information: full citation, abstract, references, citings, index terms

Interpreted languages have become increasingly popular due to demands for rapid program development, ease of use, portability, and safety. Beyond the general impression that they are "slow," however, little has been documented about the performance of interpreters as a class of applications.This paper examines interpreter performance by measuring and analyzing interpreters from both software and hardware perspectives. As examples, we measure the MIPSI, Java, Perl, and Tcl interpreters running an ...

195 ASHs: Application-specific handlers for high-performance messaging
Deborah A. Wallach, Dawson R. Engler, M. Frans Kaashoek
August 1996 **ACM SIGCOMM Computer Communication Review , Conference proceedings on Applications, technologies, architectures, and protocols for computer communications**, Volume 26 Issue 4
Additional Information:

Full text available: pdf(174.50 KB) full citation, abstract, references, citings, index terms

Application-specific safe message handlers (ASHs) are designed to provide applications with hardware-level network performance. ASHs are user-written code fragments that safely and efficiently execute in the kernel in response to message arrival. ASHs can direct message transfers (thereby eliminating copies) and send messages (thereby reducing send-response latency). In addition, the ASH system provides support for dynamic integrated layer processing (thereby eliminating duplicate message ...

196 Using CD-ROMs and local Web pages to provide course materials for distance-students

V. E. Veraart, S. L. Wright

June 1996 **Proceedings of the 1st conference on Integrating technology into computer science education**, Volume 28 , 24 Issue SI , 1-3

Full text available: pdf(385.55 KB) Additional Information: full citation, references, citings, index terms

197 Atomicity in electronic commerce

J. D. Tygar

May 1996 **Proceedings of the fifteenth annual ACM symposium on Principles of distributed computing**

Full text available: pdf(1.74 MB) Additional Information: full citation, references, citings, index terms

198 The computer science fair: an alternative to the computer programming contest

Sue Fitzgerald, Mary Lou Hines

March 1996 **ACM SIGCSE Bulletin , Proceedings of the twenty-seventh SIGCSE technical symposium on Computer science education**, Volume 28 Issue 1

Full text available: pdf(448.44 KB) Additional Information: full citation, abstract, references, index terms

Dissatisfaction with the results of programming contest events has led to the development of a new type of competitive event, a computer science fair. The computer science fair, a combination art show/science fair, is designed to attract a wider diversity of participants, to encourage creativity, and to reinforce good project development practices. Students are asked to creatively use technology to express themselves, to design new inventions, and to solve problems by submitting projects in the ...

Keywords: gender issues, programming contests, recruiting

199 Publishing online, a commercial (ad)venture

Nancy Cooke, David McAllister

February 1996 **Proceedings of the 13th annual international conference on Systems documentation: emerging from chaos: solutions for the growing complexity of our jobs**

Full text available: pdf(523.25 KB) Additional Information: full citation, references, index terms

200 The Ω key management service

Michael K. Reiter, Matthew K. Franklin, John B. Lacy, Rebecca N. Wright

January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security**

Full text available: pdf(1.37 MB) Additional Information: full citation, references, citings, index terms

Results 181 - 200 of 200 Result page: previous 1 2 3 4 5 6 7 8 9 **10**

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2005 ACM, Inc.
Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player

PORTAL
USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: The ACM Digital Library The Guide

encrypted objects

Search

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used **encrypted objects**

Found **56,840** of **154,226**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale

1 Technical poster session 1: multimedia analysis, processing, and retrieval: Security of human video objects by incorporating a chaos-based feedback cryptographic scheme

Tzouveli Paraskevi, Ntalianis Klimis, Kollias Stefanos

October 2004 **Proceedings of the 12th annual ACM international conference on Multimedia**

Full text available: pdf(241.08 KB) Additional Information: full citation, abstract, references, index terms

Security of multimedia files attracts more and more attention and many encryption methods have been proposed in literature. However most cryptographic systems deal with multimedia files as binary large objects, without taking into consideration regions of semantic information. These regions may need better protection or can be the only regions that need protection, depending on the specific application. Towards this direction, in this paper we propose a human video object encryption system ba ...

Keywords: chaos, cryptographic systems, face and body detection, human video objects, logistic map

2 A key distribution method for object-based protection

Warwick Ford, Michael J. Wiener

November 1994 **Proceedings of the 2nd ACM Conference on Computer and communications security**

Full text available: pdf(501.57 KB) Additional Information: full citation, abstract, references, index terms

In any scheme for protecting the confidentiality of data, selecting a key and encrypting the data is the easy part. The difficult part is controlling access to decryption keys. This becomes particularly significant with object-based protection, that is protection of an object, such as a file or a message, regardless of where the object is currently being stored or transferred within a distributed environment. An example of object-based protection is traditional electronic m ...

3 Towards a secure platform for distributed mobile object computing

Marc Lacoste

April 2000 **ACM SIGOPS Operating Systems Review**, Volume 34 Issue 2

Full text available: pdf(1.42 MB) Additional Information: full citation, abstract, index terms

We present some issues relevant to the design of a secure platform for distributed mobile computing, that goes beyond existing ad-hoc approaches to software mobility. This

platform aims to support wide-area computing applications such as active network infrastructures or network supervision tools. Our contribution is two-fold: the first part of the paper is a survey of the security features of a few languages and virtual machines as regards authentication, access control, and communications secu ...

4 Special section on impact of quantum technologies on networks and networking research: Quantum-noise: protected data encryption for WDM fiber-optic networks

Eric Corndorf, Chuang Liang, Gregory S. Kanter, Prem Kumar, Horace P. Yuen

October 2004 **ACM SIGCOMM Computer Communication Review**, Volume 34 Issue 5

Full text available: pdf(696.74 KB) Additional Information: full citation, abstract, references, index terms

We demonstrate high data-rate quantum-noise{protected data encryption through optical fibers using coherent states of light. Specifically, we demonstrate 650Mbps data encryption through a 10Gbps data-bearing, in-line amplified 200km-long line. In our protocol, legitimate users (who share a short secret-key) communicate using an M-ry signal set while an attacker (who does not share the secret-key) is forced to contend with the fundamental and irreducible quantum-measurement noise of coherent stat ...

Keywords: data encryption, quantum cryptography

5 Embedded applications: Encryption overhead in embedded systems and sensor network nodes: modeling and analysis

Ramnath Venugopalan, Prasanth Ganesan, Pushkin Peddabachagari, Alexander Dean, Frank Mueller, Mihail Sichitiu

October 2003 **Proceedings of the 2003 international conference on Compilers, architecture and synthesis for embedded systems**

Full text available: pdf(293.59 KB) Additional Information: full citation, abstract, references, citings, index terms

Recent research in sensor networks has raised issues of security for small embedded devices. Security concerns are motivated by the deployment of a large number of sensory devices in the field. Limitations in processing power, battery life, communication bandwidth and memory constrain the applicability of existing cryptography standards for small embedded devices. A mismatch between wide arithmetic for security (32 bit word operations) and embedded data bus widths (often only 8 or 16 bits) combi ...

Keywords: embedded systems, encryption, security, sensor networks

6 Security: Analyzing and modeling encryption overhead for sensor network nodes

Prasanth Ganesan, Ramnath Venugopalan, Pushkin Peddabachagari, Alexander Dean, Frank Mueller, Mihail Sichitiu

September 2003 **Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications**

Full text available: pdf(254.57 KB) Additional Information: full citation, abstract, references, index terms

Recent research in sensor networks has raised security issues for small embedded devices. Security concerns are motivated by the deployment of a large number of sensory devices in the field. Limitations in processing power, battery life, communication bandwidth and memory constrain the applicability of existing cryptography standards for small embedded devices. A mismatch between wide arithmetic for security (32 bit word operations) and embedded data bus widths (often only 8 or 16 bits) combined ...

Keywords: analysis, embedded systems, encryption overhead, model, sensor networks

7 Cryptographic sealing for information secrecy and authentication
David K. Gifford
April 1982 **Communications of the ACM**, Volume 25 Issue 4

Full text available: pdf(1.29 MB) Additional Information: full citation, abstract, references, citings, index terms

A new protection mechanism is described that provides general primitives for protection and authentication. The mechanism is based on the idea of sealing an object with a key. Sealed objects are self-authenticating, and in the absence of an appropriate set of keys, only provide information about the size of their contents. New keys can be freely created at any time, and keys can also be derived from existing keys with operators that include Key-And and Key-Or

Keywords: conentional crypto-systems, cryptographic sealing, key, seal, secrecy, unseal

8 Secure external references in multimedia email messages
Burkhard Wiegel
January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security**

Full text available: pdf(1.27 MB) Additional Information: full citation, references, index terms

9 Symmetric and Asymmetric Encryption
Gustavus J. Simmons
December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4

Full text available: pdf(2.23 MB) Additional Information: full citation, references, citings, index terms

10 A taxonomy for key escrow encryption systems
Dorothy E. Denning, Dennis K. Branstad
March 1996 **Communications of the ACM**, Volume 39 Issue 3

Full text available: pdf(548.67 KB) Additional Information: full citation, citings, index terms, review

11 Mathematics of computing: A Java implemented key collision attack on the data encryption standard (DES)
John Loughran, Tom Dowling
June 2003 **Proceedings of the 2nd international conference on Principles and practice of programming in Java**

Full text available: pdf(93.37 KB) Additional Information: full citation, abstract, references, index terms

A Java implementation of a key collision attack on DES suggested by Eli Biham, [1], is discussed. Storage space minimization and fast searching techniques to speed up the attack are described. We also demonstrate the suitability of Java for large data cryptographic attacks and illustrate the extensive cryptographic features of the language.

Keywords: DES, key collision attack

12 A java API for historical ciphers: an object-oriented design project
Ralph Morelli, Ralph Walde, Gregg Marcuccio
February 2001 **ACM SIGCSE Bulletin , Proceedings of the thirty-second SIGCSE technical symposium on Computer Science Education**, Volume 33 Issue 1

Full text available: pdf(185.90 KB) Additional Information: full citation, abstract, references, index terms

This paper describes a project suitable for a software engineering or object-oriented design course. The project consists of asking students to design an *application programming interface (API)* for a particular range of applications. An API-design project has several features not always found in application-design projects: It forces students to focus carefully on the distinction between the programming and the user interfaces; it provides a good justification for studying existing APIs a ...

13 A secure distributed capability based system (extended abstract)
Howard L. Johnson, John F. Koegel, Rhonda M. Koegel
October 1985 **Proceedings of the 1985 ACM annual conference on The range of computing : mid-80's perspective: mid-80's perspective**
Full text available: pdf(1.22 MB) Additional Information: full citation, references, index terms

Keywords: capability architecture, computer security, distributed system security, network encryption

14 Coding and Encryption: On error preserving encryption algorithms for wireless video transmission
Ali Saman Saman Tosun, Wu-chi Feng
October 2001 **Proceedings of the ninth ACM international conference on Multimedia**
Full text available: pdf(157.93 KB) Additional Information: full citation, abstract, references, index terms

In this paper, we describe error preserving encryption mechanisms for transmission of vido over wireless networks. One of the main problems with the secure transmission of data over wireless networks is that the bit errors that occur need to typically be sesolved *before* decryption can begin. For vido straming applications, this is unacceptable due to the general requirement that video be presented to the user in a continuous manner with low latency. In this paper, we describe a systematic ...

Keywords: video encryption, wireless video transmission

15 DISP: Practical, efficient, secure and fault-tolerant distributed data storage
Daniel Ellard, James Megquier
February 2005 **ACM Transactions on Storage (TOS)**, Volume 1 Issue 1
Full text available: pdf(148.11 KB) Additional Information: full citation, abstract, references, index terms

DISP is a practical client-server protocol for the distributed storage of immutable data objects. Unlike most other contemporary protocols, DISP permits applications to make explicit tradeoffs between total storage space, computational overhead, and guarantees of availability, integrity, and privacy on a per-object basis. Applications specify the degree of redundancy with which each item is encoded, what level of integrity checks are computed and stored with each item, and whether items are stor ...

Keywords: Distributed data storage

16 Non-reversible VHDL source-source encryption
Kevin O'Brien, Serge Maginot
September 1994 **Proceedings of the conference on European design automation**
Full text available: pdf(678.63 KB) Additional Information: full citation, references, index terms

17 Session 2: secure Web services: Validating a Web service security abstraction by typing

Andrew D. Gordon, Riccardo Pucella

November 2002 **Proceedings of the 2002 ACM workshop on XML security**

Full text available: pdf(210.31 KB) Additional Information: full citation, abstract, references, citings, index terms

An XML web service is, to a first approximation, an RPC service in which requests and responses are encoded in XML as SOAP envelopes, and transported over HTTP. We consider the problem of authenticating requests and responses at the SOAP-level, rather than relying on transport-level security. We propose a security abstraction, inspired by earlier work on secure RPC, in which the methods exported by a web service are annotated with one of three security levels: none, authenticated, or both authen ...

Keywords: Web services, authentication, remote procedure call, type systems

18 Access Control Models and Mechanisms: Cryptographic access control in a distributed file system

Anthony Harrington, Christian Jensen

June 2003 **Proceedings of the eighth ACM symposium on Access control models and technologies**

Full text available: pdf(249.24 KB) Additional Information: full citation, abstract, references, index terms

Traditional access control mechanisms rely on a reference monitor to mediate access to protected resources. Reference monitors are inherently centralized and existing attempts to distribute the functionality of the reference monitor suffer from problems of scalability.Cryptographic access control is a new distributed access control paradigm designed for a global federation of information systems. It defines an implicit access control mechanism, which relies exclusively on cryptography to provide ...

Keywords: access control, cryptography, network file systems

19 OceanStore: an architecture for global-scale persistent storage

John Kubiatowicz, David Bindel, Yan Chen, Steven Czerwinski, Patrick Eaton, Dennis Geels, Ramakrishna Gummadi, Sean Rhea, Hakim Weatherspoon, Chris Wells, Ben Zhao

November 2000 **Proceedings of the ninth international conference on Architectural support for programming languages and operating systems**, Volume 28 , 34 Issue 5 , 5

Full text available: pdf(166.53 KB) Additional Information: full citation, abstract, references, citings, index terms

OceanStore is a utility infrastructure designed to span the globe and provide continuous access to persistent information. Since this infrastructure is comprised of untrusted servers, data is protected through redundancy and cryptographic techniques. To improve performance, data is allowed to be cached anywhere, anytime. Additionally, monitoring of usage patterns allows adaptation to regional outages and denial of service attacks; monitoring also enhances performance through pro-active movement ...

20 SCONE: using concurrent objects for low-level operating system programming

Jun-ichiro Itoh, Yasuhiko Yokote, Mario Tokoro

October 1995 **ACM SIGPLAN Notices , Proceedings of the tenth annual conference on Object-oriented programming systems, languages, and applications**, Volume 30 Issue 10

Full text available: pdf(1.66 MB) Additional Information: full citation, abstract, references, citings, index terms

This paper proposes a methodology for making low-level system code of operating systems be replaceable at runtime. Our approach is to use concurrent objects as a basic programming unit for low-level system programs. To realize the different need for each type of system code and to execute these concurrent objects sufficiently efficient, we use a combination of dedicated system service layers and other implementation techniques. System service layers provide the most suitable primitive operations ...

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2005 ACM, Inc.
Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player

PORTAL USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: The ACM Digital Library The Guide

encrypted applet

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used **encrypted applet** Found **3,651** of **154,226**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown Relevance scale

1 Applications: An analysis of Internet chat systems

Christian Dewes, Arne Wichmann, Anja Feldmann

October 2003 **Proceedings of the 3rd ACM SIGCOMM conference on Internet measurement**

Full text available: pdf(630.55 KB) Additional Information: full citation, references, citings, index terms

Keywords: IRC, chat, network measurements

2 Reviewed papers: Cryptography and security protocols course for undergraduate IT students

Alaaeldin A. Aly, Shakil Akhtar

June 2004 **ACM SIGCSE Bulletin**, Volume 36 Issue 2

Full text available: pdf(340.59 KB) Additional Information: full citation, abstract, references

This paper presents an application of active learning methodologies to teach cryptography and security protocols for undergraduate IT students. This course is offered to sophomore/junior students and is based upon the recently approved Computing Curricula CC 2001 by IEEE Computer Society/ACM taskforce. We illustrate the teaching methodology to cover the security related topics such as encryption/decryption methodologies, security and protection, cryptographic algorithms and standards, and comput ...

Keywords: active learning, computing curricula, security protocols, teaching cryptographic algorithms

3 Security issues surrounding programming languages for mobile code: JAVA vs. Safe-Tcl

Stefanos Gritzalis, George Aggelis

April 1998 **ACM SIGOPS Operating Systems Review**, Volume 32 Issue 2

Full text available: pdf(1.42 MB) Additional Information: full citation, abstract, references

JAVA is claimed to be a system programming language having a number of advantages over traditional programming languages. These advantages stem from the fact that it is a platform - independent language, thus promising truly network oriented computing as long as a nearly universal system for distributing applications. On the other hand, although

being an interpreted, much simpler, scripting language, Safe-Tcl was proposed as an executable contents type of MIME and thus as the standard language f ...

4 Web and IP based design: IP delivery for FPGAs using Applets and JHDL
Michael J. Wirthlin, Brian McMurtrey
June 2002 **Proceedings of the 39th conference on Design automation**

Full text available: pdf(198.07 KB) Additional Information: full citation, abstract, references, index terms

This paper introduces an FPGA IP evaluation and delivery system that operates within Java applets. The use of such applets allows designers to create, evaluate, test, and obtain FPGA circuits directly within a web browser. Based on the JHDL design tool, these applets allow structural viewing, circuit simulation, and netlist generation of application-specific circuits. Applets can be customized to provide varying levels of IP visibility and functionality as needed by both customer and vendor.

Keywords: FPGA, JHDL, applet, intellectual property

5 Gauging the risks of internet elections
Deborah M. Phillips, Hans A. von Spakovsky
January 2001 **Communications of the ACM**, Volume 44 Issue 1

Full text available: pdf(159.11 KB) html(35.52 KB) Additional Information: full citation, references, index terms

6 The case for internet voting
Joe Mohen, Julia Glidden
January 2001 **Communications of the ACM**, Volume 44 Issue 1

Full text available: pdf(158.11 KB) html(35.34 KB) Additional Information: full citation, references, citings, index terms

7 World Wide Web based grades management
Atsuyuki Morishima, Hiroyuki Kitagawa
April 1997 **Proceedings of the 1997 ACM symposium on Applied computing**

Full text available: pdf(388.64 KB) Additional Information: full citation, index terms

Keywords: Internet, JAVA, class management, grading system

8 Teaching with Java: Using Java to increase active learning in programming courses
Aoileann nic Gearailt
June 2002 **Proceedings of the inaugural conference on the Principles and Practice of programming, 2002 and Proceedings of the second workshop on Intermediate representation engineering for virtual machines, 2002**

Full text available: pdf(467.12 KB) Additional Information: full citation, abstract, references, index terms

Introductory courses in Programming often have many objectives, some explicit and some implicit. Increased pressure to cater for a wide range of abilities and backgrounds within the same class-group leads to a conflict between the need to lay solid foundations for the student who will eventually make a career as a software developer, and the need to provide a useful and rewarding learning experience which imparts some understanding of the

principles of programming to the others. This paper propo ...

9 Security issues in distributed software
Richard A. Kemmerer
November 1997 **ACM SIGSOFT Software Engineering Notes , Proceedings of the 6th European conference held jointly with the 5th ACM SIGSOFT international symposium on Foundations of software engineering**, Volume 22 Issue 6
Full text available: pdf(632.79 KB) Additional Information: full citation, references, index terms

10 Teaching computer organization/architecture with limited resources using simulators
Gregory S. Wolffe, William Yurcik, Hugh Osborne, Mark A. Holliday
February 2002 **ACM SIGCSE Bulletin , Proceedings of the 33rd SIGCSE technical symposium on Computer science education**, Volume 34 Issue 1
Full text available: pdf(455.40 KB) Additional Information: full citation, abstract, references, citings

As the complexity and variety of computer system hardware increases, its suitability as a pedagogical tool in computer organization/architecture courses diminishes. As a consequence, many instructors are turning to simulators as teaching aids, often using valuable teaching/research time to construct them. Many of these simulators have been made freely available on the Internet, providing a useful and time-saving resource for other instructors. However, finding the right simulator for a particula ...

11 Computer security and impact on computer science education
T. Andrew Yang
April 2001 **Journal of Computing Sciences in Colleges , Proceedings of the sixth annual CCSC northeastern conference on The journal of computing in small colleges**, Volume 16 Issue 4
Full text available: pdf(160.91 KB) Additional Information: full citation, abstract, references, citings, index terms

The integration of computer security into existing Computer Science undergraduate education is an urgent and complicated task. With the increasing risk of computer intrusion, computer crimes and information wars, Computer Science educators bear the responsibility of cultivating a new generation of graduates who are aware of computer security related issues and are equipped with proper knowledge and skills to solve the problems. The task of integrating computer security into existing Computer ...

12 Architecture and performance of server-directed transcoding
Björn Knutsson, Honghui Lu, Jeffrey Mogul, Bryan Hopkins
November 2003 **ACM Transactions on Internet Technology (TOIT)**, Volume 3 Issue 4
Full text available: pdf(927.92 KB) Additional Information: full citation, abstract, references, citings, index terms, review

Proxy-based transcoding adapts Web content to be a better match for client capabilities (such as screen size and color depth) and last-hop bandwidths. Traditional transcoding breaks the end-to-end model of the Web, because the proxy does not know the semantics of the content. *Server-directed transcoding* preserves end-to-end semantics while supporting aggressive content transformations.We show how server-directed transcoding can be integrated into the HTTP protocol and into the implementat ...

Keywords: HTTP, proxy, transcode, web

13 Data security for Web-based CAD

Scott Hauck, Stephen Knol
May 1998 **Proceedings of the 35th annual conference on Design automation - Volume 00**

Full text available: pdf(198.79 KB) Publisher Site Additional Information: full citation, abstract, references, citings, index terms

Internet-based computing has significant potential for improving most high-performance computing, including VLSI CAD. In this paper we consider the ramifications of the Internet on electronics design, and develop two models for Web-based CAD. We also investigate the security of these systems, and propose methods for protection against threats both from unrelated users, as well as from the CAD tools and tool developers themselves. These techniques provide methods for hiding unnecessary infor ...

Keywords: Internet, Web-based CAD, data security, encryption

14 Security for Web Applications and P2P: Certified email with a light on-line trusted third party: design and implementation
Martín Abadi, Neal Glew
May 2002 **Proceedings of the eleventh international conference on World Wide Web**

Full text available: pdf(189.19 KB) Additional Information: full citation, abstract, citings, index terms

This paper presents a new protocol for certified email. The protocol aims to combine security, scalability, easy implementation, and viable deployment. The protocol relies on a light on-line trusted third party; it can be implemented without any special software for the receiver beyond a standard email reader and web browser, and does not require any public-key infrastructure.

15 HyperNews: a MEDIA application for the commercialization of an electronic newspaper
Jean-Henry Morin, Dimitri Konstantas
February 1998 **Proceedings of the 1998 ACM symposium on Applied Computing**

Full text available: pdf(2.74 MB) Additional Information: full citation, references, index terms

Keywords: agents, copyright protection, electronic publishing

16 SAFE-OPS: An approach to embedded software security
Joseph Zambreno, Alok Choudhary, Rahul Simha, Bhagi Narahari, Nasir Memon
February 2005 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 4 Issue 1

Full text available: pdf(556.27 KB) Additional Information: full citation, abstract, references, index terms

The new-found ubiquity of embedded processors in consumer and industrial applications brings with it an intensified focus on security, as a strong level of trust in the system software is crucial to their widespread deployment. The growing area of *software protection* attempts to address the key steps used by hackers in attacking a software system. In this paper, we introduce a unique approach to embedded software protection that utilizes a hardware/software codesign methodology. Results d ...

Keywords: HW/SW codesign, Software protection

17 Special session on mobile computing #1: Developing smart card applications using the OpenCard Framework

Mark Burge
April 2004 **Proceedings of the 42nd annual Southeast regional conference**

Full text available: pdf(428.99 KB) Additional Information: full citation, abstract, references, index terms

Smart cards provide a compact, secure, and widely used method for identifying ourselves and authenticating our transactions. With their increasing incorporation into credit cards and the cellular industries move toward smart card based GSM networks, they are positioned to become truly pervasive. Unfortunately, until now, teaching smart card development required expensive, specialized hardware and software as well as detailed, and usually proprietary, knowledge of the hardware and operating syste ...

Keywords: JCOP, Java Card, Mobile Computing, OpenCard Framework, Smart Cards, design patterns, pervasive computing

18 Getting your network ready for year 2000
Kevin Reichard
May 1998 **netWorker**, Volume 2 Issue 2

Full text available: pdf(497.99 KB) Additional Information: full citation, index terms

19 DOS protection: Using graphic turing tests to counter automated DDoS attacks against web servers
William G. Morein, Angelos Stavrou, Debra L. Cook, Angelos D. Keromytis, Vishal Misra, Dan Rubenstein
October 2003 **Proceedings of the 10th ACM conference on Computer and communications security**

Full text available: pdf(256.83 KB) Additional Information: full citation, abstract, references, citings, index terms

We present WebSOS, a novel overlay-based architecture that provides guaranteed access to a web server that is targeted by a denial of service (DoS) attack. Our approach exploits two key characteristics of the web environment: its design around a human-centric interface, and the extensibility inherent in many browsers through downloadable "applets." We guarantee access to a web server for a large number of *previously unknown* users, without requiring pre-existing trust relationships between ...

Keywords: Java, graphic turing tests, web proxies

20 Educational environments: Resource management portal for laboratories using real devices on the Internet
Stefan Zimmerli, Marc-Alain Steinemann, Torsten Braun
July 2003 **ACM SIGCOMM Computer Communication Review**, Volume 33 Issue 3

Full text available: pdf(343.16 KB) Additional Information: full citation, abstract, references, index terms

Internet-based distance learning is slowly gaining new territories and substituting current teaching methodologies. However, distance learning not only consists of transferring documents to web pages, but also of developing new concepts, methods, and implementation architectures. This article presents concepts and implementation issues for an example remote hands-on networking laboratory. The described course gives access to real network hardware via the Internet. In particular, authentication, ...

Keywords: computer networks laboratory, distance learning, hands-on training, resource management

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2005 ACM, Inc.
Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player